Implementing a Honeynet in Azure

**Objective**: The purpose of these lab is to demonstrate the integration of Azure Sentinel, a cloud native Security Information and Event Management (SIEM) solution, with a virtual machine (VM) hosted on Microsoft Azure. Specifically, the lab will focus on inspecting failed RDP logs using PowerShell to extract IP addresses from windows event viewer to transfer data to a third-party API and the API will derive the latitude, longitude, state, and country to forward back into the virtual machine, which will create a custom log with geographic data in it. The log file will be forwarded into Azure Sentinel for centralized monitoring and analysis, also to create world map plotting where brute force attacks are coming from.

A white rectangular with blue and red symbols

Description automatically generated with medium confidence

**Setting up the Azure Environment**

**Virtual Machine**

In Azure portal, a virtual machine will be created to be exposed to the internet to act as a honeypot for various threat actors around the world attempting to gain unauthorize access. A screenshot of a computer

Description automatically generated

The VM’s network settings and firewall will be configured essentially to be open to the public internet by implementing an inbound rule that allows all network traffic into the VM. The point of the firewall rule is to make the VM very discoverable quickly so threat actors across the internet can see the VM is online and vulnerable to attacks, to then subsequently start attacking. Once the VM is launched with a windows 10 OS the firewall settings will be turned off as well. This is not an ideal configuration of a VM, but for the lab, it will be configured to create an enticing honeypot which’s purpose is to attract and detect malicious activity. A screenshot of a computer

Description automatically generated

**Log Analytics Workspace**

Next in Azure portal, log analytics workspace will be created to ingest windows event logs into Azure Sentinel (SIEM). Creation of custom logs that contains geographic information to discover where attackers are coming from will also be created. To accomplish this a log analytics, log analytics workspace will be created and connected to the VM to store logs generated, then the SIEM Azure Sentinel will connect to the workspace to be able to display geodata on the map.

A screenshot of a computer

Description automatically generated

**Azure Sentinel**

Azure sentinel will be generally used to visualize the attack data, the configuration is relatively easy, consisting of creating a new sentinel workspace and then connecting it to Log analytics workspace created above.

**API for IP Geolocation**

A screenshot of a computer

Description automatically generatedAfter the creation of the Azure Environment which consist of the honeypot VM, Log analytics workspace and Sentinel, next will be to set up the API for IP geolocation. The Windows Event Viewer is a tool in Microsoft Windows operating systems that allows users to view and manage the event logs on a computer. Event logs are records of significant events, errors, and warnings generated by the operating system, applications, and system components. Using event viewer, focusing on security event id 4625, which logs IP addresses of any other systems attempting to gain access to the VM using RDP. Event Viewer does not log any data indicative of where the attempts to gain access are coming from like countries, states, longitude, and latitude. To get geolocation data, programmatically using PowerShell, IP addresses will be extracted to be used in a third-party API called ipgeolocation.io to produce more information like country, state, longitude, and latitude. Using the API and a PowerShell script, whose purpose is to perpetually run to grab all events of failed attempts to log into the VM, grab their IP addresses to get geodata for them, to then store them into a log file. A screenshot of a computer

Description automatically generated

A close-up of a screen

Description automatically generated

**Custom Log Creation**

Using the log file created by the PowerShell script, the log file will be imported into log analytic workspace by connecting the path location of the log file on the VM, so new raw data generated can be imported into log analytics. In log analytics the next step will be to train log analytics using a script that organizes the data extracted into correct columns.A screenshot of a computer

Description automatically generated

**Map Configuration**

In Azure Sentinel, a new workbook will be created, using the same query script to organize data in the custom log section, it will be used in this section to properly plot locations of failed RDP attempts on a word map. After querying data, it gives the ability to plot by Longitude/Latitude or Country, sizing by the number of events occurred, both results will be displayed.A screenshot of a computer

Description automatically generated

**A map of the world with colored circles

Description automatically generatedA map of the world with different colored circles

Description automatically generatedAttacks**

To the left are the results of attacks plotted by country, and at the bottom are results of attacks plotted by Longitude/Latitude. After 15 hours of the virtual machine being operational, these results were recorded.

**Conclusion**

In conclusion, this SIEM lab leveraging Azure Sentinel, a virtual machine configured as a honeypot, and PowerShell for API interaction has provided a comprehensive exploration into modern cybersecurity practices. By seamlessly integrating Azure Sentinel, a robust cloud native SIEM solution, with a virtual machine honeypot architecture, the lab enabled the monitoring and analysis of security events within a controlled environment. The utilization of PowerShell scripting further demonstrated the automation capabilities for extracting IP geolocation data through an API, showcasing the practical applications of scripting in cybersecurity operations. This lab also showcase the fact that any device connected to the internet that somehow has a public routable Ip address; there will be attempts to break into the device by threat actors around the world on the internet, also using default configurations like Admin or Administration for usernames and password should not be default practice for anyone especially for organizations, looking at the logs generated below, Admin and Administrator was one of the most used usernames used to attempt to gain access to the VM. A close-up of a computer screen

Description automatically generated

The use of Multi-factor authentication, restricting RDP access to the general internet, secure configuration, network segmentation, continuous monitoring, and the use of strong passwords should be a must especially for organizations.